BANWO & IGHODALO

DATA PROTECTION AS A CULTURE - MORE THAN THE MANDATORY ANNUAL AUDIT

AUGUST 14, 2024

More than ever, compliance with data protection obligations has become a critical concern for organizations across various industries in today's digital age. With the advent of stringent regulations such as the GDPR, the Nigeria Data Protection Act (the "**NDPA**")[1] and the Nigeria Data Protection Regulation (the "**NDPR**")[2], data processing entities are compelled at the risk of stiff penalties to prioritize safeguarding personal data and ensuring that the privacy rights of individuals are respected and protected. While conducting an annual data protection audit[3] and submitting compliance returns[4] is undoubtedly an essential aspect of data protection compliance, it is just one piece of the puzzle in the larger framework of ensuring robust data protection practices.

It is instructive in this regard to note that the NDPA imposes an obligation on all data controllers and data processors to use appropriate technical and organizational measures to ensure confidentiality, integrity, and availability of personal data[5]. By imposing a duty of care on data controllers and data processors in respect of data processing and requiring them to demonstrate accountability in respect of the principles contained in the NDPA[6], the NDPA has lifted data protection compliance beyond mere regulatory checkboxes. It now encompasses a holistic approach towards managing personal data throughout its lifecycle. The mandatory annual audits only provide a snapshot of an entity's level of compliance at a specific point in time. True data protection compliance requires continuous vigilance.

Organizations that look to establishing a viable data protection culture will need to take the following minimum measures:

- **Appointment of a Data Protection Officer (DPO):** Appointing a DPO fosters internal awareness and acts as a central point of contact for the data subjects[7] and the regulator – Nigeria Data Protection Commission (NDPC). DPOs are obligated to raise awareness of data protection within their various organizations, and amongst their vendors, partners and third-party service providers[8]. They drive the data protection culture and act as the go-to person and subject matter experts in the relevant organizations.

- **Establishment and Implementation of a Data Governance Framework**: Developing a robust and formidable data governance framework is foundational to attaining a level of compliance to data protection laws and principles. This framework should outline clear policies, procedures, and accountability measures for the collection, processing, storage, transfer and disposal of personal data[9] within the organization. It is important to note that the implementation of such data protection measures outlined in the framework is also critical to effecting true compliance.

1. Nigeria Data Protection Act (NDPA) 2023
2. Nigeria Data Protection Regulation (NDPR) 2019
3. NDPR Article 4.1 (4-7)
4. NDPA Section 61(2)(g)
5. Section 24(2), NDPA
6. Section 24(3), NDPA
7. "Data subject" means an individual to whom personal data relates.
8. NDPA Section 32.
9. "Personal data" means any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual.

important to note that the implementation of such data protection measures outlined in the framework is also critical to effecting true compliance.

- **Risk Assessment and Mitigation**: Conducting regular risk assessments to identify potential vulnerabilities and threats to personal data in an organization's possession is essential. Organizations should regularly conduct Data Protection Impact Assessments (DPIAs)[10] to identify risks associated with a new processing activity, particularly where the processing of personal data may likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purposes. In addition, the entity should implement appropriate security measures and controls to effectively mitigate identified risks.

- **Privacy by Design and Default**: Integrating privacy by design and default principles into business processes and systems ensures that data protection considerations are embedded from the onset. This may involve adopting Privacy-Enhancing Technologies (PETs) and practices to minimize or eliminate the risks associated with collection and processing of personal data. PETs adopt engineered systems such as secure multiparty computations, homomorphic encryption, anonymisation, differential privacy, mix networks, anonymous digital credentials etc., that provide adequate levels of privacy for personal data[11]. They are information security techniques that enhance privacy, protect and reduce the risk of personal data exposure to unauthorized third parties[12]. They incorporate primary data protection principles by minimising the usage of personal information, maximising data security, and empowering data subjects.

- **Employee Training and Awareness**: Employees play a pivotal role in data protection compliance. Providing comprehensive training programs and raising awareness among staff about their responsibilities regarding data protection is crucial. This includes educating employees about the importance of confidentiality, data handling best practices, and how to respond to data breaches effectively.

- **Data Subject Rights Management**: Ensuring recognition of and fostering an environment for the exercise of data subject rights, such as the right to access, rectify, and delete personal data, is also a major aspect of establishing a viable data protection culture. Organizations should have mechanisms in place to promptly respond to such requests and demonstrate accountability in handling individuals' personal data.

- **Data Breach Preparedness and Incident Response Procedures**: In spite of best efforts, data breaches may still occur. Being prepared to respond swiftly and effectively to data breaches is paramount. Organizations should have robust incident response plans in place, including procedures for notifying regulatory authorities and affected individuals in accordance with legal requirements.

- **Continuous Monitoring and Improvement**: Monitoring and maintaining compliance to data protection best practices is a continuous journey. Organizations should incessantly observe their data protection practices, conduct periodic reviews and audits, and implement corrective measures as necessary to address any deficiencies and adapt to evolving regulatory requirements and cybersecurity threats.

- **Periodic Review of Data Protection Framework:** Organizations should undertake regular review of their data protection framework. This entails a review of privacy notices to ascertain whether the notices are up to date, contain all information

10 "Data privacy impact assessment" is a process designed to identify the risks and impact of the envisaged processing of personal data, and it comprises — (a) a systematic description of the envisaged processing and its purpose, including the legitimate interest pursued by the data controller, data processor, or third party ; (b) an assessment of the necessity and proportionality of the processing in relation to the purposes for which the personal data would be processed ; (c) an assessment of the risks to the rights and freedoms of a data subject ; and (d) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data, taking into account the rights and legitimate interests of a data subject and other persons concerned.

11. IAPP, "Privacy Program Management" 3rd Edition, Ch. 5, p. 163.

12. IBM, "Privacy Enhancing Technologies for Regulatory Compliance" available at:

required, meet the requirements of the law and are visible at every collection point for personal data within the organization. This will also extend to the periodic re-examination of the lawful bases on which processing of data takes place to ascertain whether the organization may still rely on those bases for processing or a review of personal data held by them to ascertain whether there has been any change in the type or use of the data, and whether there is a need to review/ amend/ delete the personal data. It also involves a periodic review of privacy and cybersecurity protocols such as analysis of the manner in which such data subject requests are dealt with, the timeline for meeting such requests and key-man risks in the data protection department.

Conclusion

Data protection compliance is not a one-time event; it is a continuous process lasting the lifetime of the business. By adopting a holistic approach that goes beyond annual audits and periodic filings, organizations can ensure they are in compliance with their legal obligations and safeguarding the personal data entrusted to them. This not only mitigates risks, but also fosters trust and a competitive advantage in the Nigerian market. In addition, the NDPC now has the power to take several enforcement actions, including ordering a data controller or data processor to pay compensation to a data subject, who has suffered injury, loss, or harm as a result of a violation, ordering the data controller or data processor to account for the profits realized from the violation, or imposing a penalty or remedial fee which may rise to 2% of a data controller or processor's annual gross revenue in a financial year[13]. Thus, failure to establish a vibrant and effective data protection system can prove costly to an organization, particularly where it is found to have breached its data protection compliance obligations which has resulted in significant loss or risk to the rights of individuals.

Data protection compliance entails more than conducting the annual audit. It requires a proactive and comprehensive approach that encompasses various elements, including governance, risk management, employee training, and incident response. By fostering a culture of respect for data protection, organizations can effectively safeguard personal data, earn the trust of their customers, and mitigate regulatory and reputational risks in an increasingly data-driven world.

DISCLAIMER: This article is intended to provide a general guide to the subject matter and does not by itself constitute legal advice to readers. Specialist advice should be sought about readers' specific circumstances.

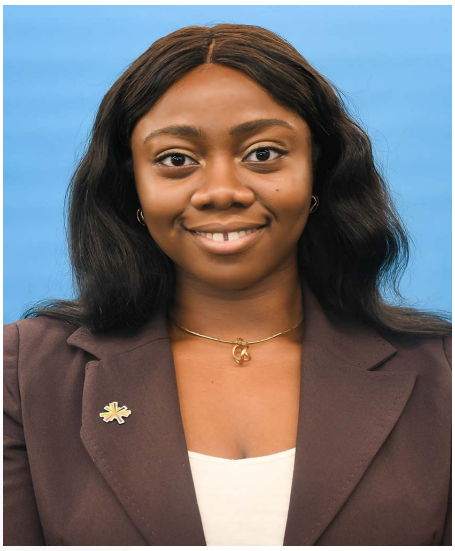
For further information, kindly contact our **Data Protection Team** at DPT@banwo-ighodalo.com

13. Nigeria's data privacy violators fined N400 million, says NDPC < https://gazettengr.com/nigerias-data-privacy-violators-fined-n400-million-says-ndpc/>

Olumide Osundolire

Partner

E: oosundolire@banwo-ighodalo.com



Vanessa Obi

Associate

E: vobi@banwo-ighodalo.com